кожного учасника процесу запропоновано використання системи сертифікації з унікальним сертифікатом для кожного POS терміналу.

Підрахунок ризиків щодо використання кожного методу передачі даних від POS терміналу до процесингу, згідно з рекомендаціями Національного Банку України, буде завданням наступного дослідження.

Список використаної літератури: ***1.*** *Alan G. Konheim Computer security and cryptography / Alan G. Konheim - John Wiley & Sons, Inc., 2007 - p. 542.* ***2.*** *PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) Version 3.0 is active from January 1, 2014.* ***3.*** *К. Г. Явлинский «Динамическая модель банковской сети» / Кирилл Григорьевич Явлинский – 2-е издание, исправленное и дополненное -из-во ДМК Фин., 2013 – 480 с.* ***4.*** *СОУ Н НБУ 65.1 СУІБ 1.0:2010 МЕТОДИ ЗАХИСТУ В БАНКІВСЬКІЙ ДІЯЛЬНОСТІ. СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. ВИМОГИ (ISO/IEC 27001:2005, mod)* ***5.*** *Carlisle Adams Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations / Carlisle Adams, Steve Lloyd, Macmillan Technical Publishing 1999 – p. 296.* ***6.*** *Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації" випуск 2(26) 2014 с.87-97 Шаповал М. В. Порівняльний аналіз методів захисту даних pos-термінального трафіку*

Юрій Васильєв
ДержНДІ Спецзв'язку

УДК 004.056

КЛАСИФІКАЦІЯ ТА АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В КЛЮЧОВИХ СИСТЕМАХ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація: **Наведено класифікацію загроз інформаційній безпеці систем управління ключових систем інформаційної інфраструктури та методи їх аналізу.**
Summary: **The classification and methods of analysis of threats to information security management systems key of information infrastructure systems.**
Ключові слова: **Загрози, інформація, інформаційна безпека, ключові системи інформаційної інфраструктури**

I Вступ

Більшість сучасних систем управління (СУ) ключовими системами інформаційної інфраструктури (КСІІ) являє собою територіально розподілені системи, які взаємодіють між собою даними (ресурсами) та управлінням (подіями) локальних обчислювальних мереж (ЛОМ) та окремих ЕОМ.

У розподілених СУ КСІІ можливі всі характерні для локально розташованих (централізованих) обчислювальних систем способи несанкціонованого втручання в їх роботу і доступу до інформації, що обробляється. Крім того, для них є і специфічні канали вторгнення в систему і несанкціонованого доступу до інформації, наявність яких пояснюється низкою їх особливостей.

Основні особливості розподілених СУ КСІІ:

територіальна розподіленність компонентів СУ і наявність інтенсивного обміну інформацією між ними;

широкий спектр способів подання, зберігання і протоколів передачі інформації, що використовуються;

інтеграція даних різного призначення, що належать різним суб'єктам, в рамках єдиних баз даних і, навпаки, розміщення необхідних деяким суб'єктам даних у різних віддалених вузлах (базах даних) мережі;

відокремлення власників даних від фізичних структур і місця розміщення даних;

використання режимів розподіленої обробки даних;

участь у процесі автоматизованої обробки інформації великої кількості користувачів і персоналу різних категорій;

безпосередній і одночасний доступ до ресурсів (в тому числі і інформаційних) великого числа користувачів (суб'єктів) різних категорій;

високий ступінь різнорідності задіяних засобів обчислювальної техніки і зв'язку, а також їх програмного забезпечення;

відсутність спеціальних засобів захисту в більшості типів технічних засобів, які використовуються в СУ КСІІ.

II Уразливість основних структурно-функціональних елементів розподілених СУ КСІІ

Як правило СУ КСІІ складаються з наступних основних структурно-функціональних елементів:

робочих станцій - окремих електронно-обчислювальних машин (далі – ЕОМ) або терміналів мережі, на яких реалізуються автоматизовані робочі місця користувачів (абонентів, операторів);

серверів (служб файлів, друку, баз даних тощо) не виділених (або виділених, тобто не суміщених з робочими станціями) високопродуктивних ЕОМ, призначених для реалізації функцій зберігання, друку даних, обслуговування робочих станцій мережі і т. п. дій;

мережевих пристроїв (маршрутизаторів, комутаторів, шлюзів, центрів комутації пакетів, комунікаційних ЕОМ) – елементів, що забезпечують з'єднання декількох мереж передачі даних, або декількох сегментів однієї і тієї ж мережі, можливо мають різні протоколи взаємодії;

каналів зв'язку (локальних, телефонних, з вузлами комутації і т. д.).

Робочі станції є найбільш доступними компонентами мереж і саме з них можуть бути вжиті найбільш численні спроби вчинення несанкціонованих дій. З робочих станцій здійснюється управління процесами обробки інформації, запуск програм, введення і коректування даних, на дисках робочих станцій можуть розміщуватися важливі дані і програми обробки. На монітори та друкуючи пристрої робочих станцій виводиться інформація при роботі користувачів (операторів), що виконують різні функції і мають різні повноваження з доступу до даних і інших ресурсів системи. Саме на робочих станціях здійснюється введення імен і паролів користувачами. Тому робочі станції повинні бути надійно захищені від доступу сторонніх осіб та містити засоби розмежування доступу до ресурсів з боку задекларованих користувачів, що мають різні повноваження. Крім того, засоби захисту повинні запобігати порушенням нормальної настройки (конфігурації) робочих станцій і режимів їх функціонування, викликані ненавмисним втручанням недосвідчених (неуважних) користувачів

Особливого захисту потребують такі привабливі для зловмисників елементи мереж як сервери і мережеві пристрої. Перші – як концентратори великих обсягів інформації, другі – як елементи, в яких здійснюється перетворення (можливо через відкриту, незашифровану форму подання) даних при узгодженні протоколів обміну в різних ділянках мережі.

Сприятливою для підвищення безпеки серверів і мережевих пристроїв обставиною є наявність можливостей їх надійного захисту фізичними засобами і організаційними заходами в силу їх виділення, що дозволяє скоротити до мінімуму число осіб з персоналу, які мають безпосередній доступ до них. Іншими словами, безпосередні випадкові впливи персоналу і навмисні локальні дії зловмисників на виділені сервери і мережеві пристрої можливо вважати малоймовірними. Але, все більш поширеними стають масовані атаки на сервери і мережеві пристрої (а так само і на робочі станції) з використанням засобів віддаленого доступу. Тут зловмисники, насамперед, можуть шукати можливості вплинути на роботу різних підсистем робочих станцій, серверів і мережевих пристроїв, використовуючи недоліки протоколів обміну даними і засобів розмежування віддаленого доступу до ресурсів і системних таблиць. Використовуватися можуть всі можливості і засоби, від стандартних (без модифікації компонентів) до підключення спеціальних апаратних засобів (канали, як правило, слабо захищені від підключення) та застосування спеціалізованих програм для подолання системи захисту.

Наведене вище не значить, що не буде спроб впровадження апаратних і програмних закладок в самі мережеві пристрої і сервери, які відкривають широкі додаткові можливості з несанкціонованого віддаленого доступу. Закладки можуть бути впроваджені як з віддалених станцій (за допомогою вірусів чи іншим способом), так і безпосередньо в апаратуру і програми серверів при їх ремонті, обслуговуванні, модернізації, перехід на нові версії програмного забезпечення, зміні обладнання.

Канали і засоби зв'язку також потребують захисту. У силу великої просторової протяжності ліній зв'язку (через неконтрольовану або слабо контрольовану територію) практично завжди існує можливість підключення до них, або втручання в процес передачі даних [1,2].

III Поняття загрози та її основні властивості

Аналіз засад забезпечення інформаційної безпеки дозволяє зробити висновок про те, що поняття «забезпечення інформаційної безпеки» включає об'єкти інформаційної безпеки, загрози об'єктам інформаційної безпеки та діяльність по захисту цих об'єктів, засновану на сукупності сил, засобів, способів і методів забезпечення інформаційної безпеки.

Головними цілями діяльності щодо забезпечення інформаційної безпеки є ліквідація загроз об'єктам інформаційної безпеки та мінімізація можливого збитку, який може бути нанесений внаслідок реалізації даних загроз.

Загроза – одне з ключових понять у сфері забезпечення інформаційної безпеки. Загроза об'єкту інформаційної безпеки є сукупність факторів і умов, що виникають у процесі взаємодії різних об'єктів (їх елементів) і здатних чинити негативний вплив на конкретний об'єкт інформаційної безпеки. Негативні впливи розрізняються за характером завдання шкоди, а саме: за ступенем зміни властивостей об'єкта безпеки і можливості ліквідації наслідків прояви загрози.

До найбільш важливих властивостей загрози відносяться вибірковість, передбачуваність та шкідливість. Вибірковість характеризує націленість загрози на нанесення шкоди тим чи іншим конкретним властивостям об'єкта безпеки. Передбачуваність характеризує наявність ознак виникнення загрози, що дозволяють заздалегідь прогнозувати можливість появи загрози і визначати конкретні об'єкти безпеки, на які вона буде спрямована. Шкідливість характеризує можливість нанесення шкоди різної тяжкості об'єкту безпеки. Шкода, як правило, може бути оцінена вартістю витрат на ліквідацію наслідків прояви загрози або на запобігання її появи.

Необхідно виділити два найбільш важливих типу загроз:

намір завдати шкоди, яке з'являється у вигляді оголошеного мотиву діяльності суб'єкта;

можливість нанесення шкоди - існування достатніх для цього умов і факторів.

Особливість першого типу загроз полягає в невизначеності можливих наслідків, неясності питання про наявність у загрозливого суб'єкта сил і засобів, достатніх для здійснення наміру.

Можливість нанесення шкоди полягає в існуванні достатніх для цього умов і факторів. Особливість загроз даного типу полягає в тому, що оцінка потенціалу сукупності факторів, які можуть слугувати перетворенню цих можливостей і умов на шкоду, може бути здійснена тільки власне суб'єктами загроз.

Між загрозою і небезпекою нанесення шкоди завжди існує стійкий причинно-наслідковий зв'язок.

Загроза завжди породжує небезпеку. Небезпеку також можна представити як стан, в якому знаходиться об'єкт безпеки внаслідок виникнення загрози цьому об'єкту. Головна відмінність між ними полягає в тому, що небезпека є властивістю об'єкта інформаційної безпеки і характеризує його здатність протистояти прояву загроз, а загроза – властивістю об'єкта взаємодії або знаходяться у взаємодії елементів об'єкта безпеки, які виступають як джерело загроз. Поняття загрози має причинно-наслідковий зв'язок не тільки з поняттям небезпеки, а й з можливою шкодою як наслідком негативної зміни умов існування об'єкта. Можлива шкода визначає величину небезпеки.

IV Класифікація загроз інформаційній безпеці СУ КСІІ

За результатами реалізації загроз інформаційній безпеці СУ КСІІ може бути порушена конфіденційність (витік, перехоплення, зняття, копіювання, розкрадання, розголошення), цілісність (втрата, знищення, модифікація) і доступність (блокування) інформації. При цьому порушення цілісності та (або) доступності інформації в СУ КСІІ може призвести до порушення достовірності та своєчасності результатів її функціонування аж до відмови системи.

Класифікація загроз може бути проведена за безліччю ознак. Найбільш поширені з них наведені в таблиці 1 [3].

Таблиця 1 – Класифікація загроз

Критерії загрози	Вид загрози
За видом властивості інформації, що порушується	загрози конфіденційності (витік, перехват, зняття, копіювання, викрадання, розголошення); загрози цілісності (втрата, знищення, модифікація); загрози доступності (блокування);
За характером порушення	порушення конфіденційності даних; порушення працездатності серверів, мережевого обладнання, робочих станцій; незаконне втручання у функціонування серверів, мережевого обладнання, робочих станцій, тощо;
За тяжкістю порушення	незначні помилки; дрібне хуліганство; серйозний злочин / природні і техногенні катастрофи;
За передбаченням наслідків порушника	умисне порушення; ненавмисне порушення;
За мотивацією	зловмисне порушення; незловмисне порушення;

За закінченістю	закінчені; незакінчені;	
За об'єктом дії	загрози, націлені на всю інформаційну систему; загрози, націлені на окремі компоненти СУ КСІІ;	
За причиною виникнення	загрози, які виникли через недостачу засобів технічного захисту; загрози, які виникли через недостачу організаційних заходів;	
За походженням	антропогенні; техногенні; природні;	
За розміром нанесеної шкоди	незначні; значні; критичні;	
За типовими об'єктами інформатизації	загрози безпеці інформації для СУ на базі автономної ЕОМ (без підключення до обчислювальної мережі); загрози безпеці інформації для СУ на базі локальної обчислювальної мережі (без підключення до розподіленої обчислювальної мережі); загрози безпеці інформації для СУ, підключеної до розподіленої обчислювальної мережі;	
За способом реалізації загроз безпеці інформації	1) загрози спеціальної дії на інформацію: механічної; хімічної; акустичної; біологічної; радіаційної; термічної; електромагнітної (електричні імпульси, електромагнітні випромінювання, магнітне поле);	
	2) загрози НСД в СУ КСІІ	
	3) загрози витоку інформації технічними каналами:	
	по радіоканалу; по електричному каналу; по оптичному каналу; по змішаним (параметричним) каналам;	загрози витоку по каналам ПЕМВН;

Класифікація загроз НСД в СУ КСІІ може бути проведена за ознаками, які наведені у таблиці 2 [3].

Таблиця 2 – Класифікація загроз НСД в СУ КСІІ

Критерії загрози	Вид загрози
За джерелом загрози	1) створені порушником: внутрішнім; зовнішнім;
	2) створені апаратною закладкою: вбудованою; автономною;
	3) створені шкідливими програмами: програмні закладки типу «Троянський кінь»; програмні віруси; шкідливі програми, що поширюються мережею (мережеві черви); інші шкідливі програми для здійснення НСД;
За використаною вразливістю системи	з використанням вразливості програмного забезпечення; з використанням вразливості, викликаної наявністю апаратної вкладки в СУ КСІІ; з використанням вразливості, пов'язаної з реалізацією протоколів мережевої взаємодії і каналів передачі даних; з використанням вразливості, викликаної недоліками організації технічного захисту інформації від НСД;

	з використанням вразливості системи захисту інформації; з використанням вразливості програмно-апаратних засобів при збоях і позаштатних ситуаціях;
За об’єктом взаємодії	1) НСД до інформації, яка обробляється на ЕОМ (вузли обчислювальної мережі): на відчужених носіях інформації; на вбудованих носіях довготривалого зберігання інформації; у засобах обробки і зберігання оперативної інформації; у засобах (портах) вводу (виводу) інформації;
	2) НСД до інформації залежно від її рівня мережевої взаємодії: на фізичному рівні; на канальному рівні; на мережевому рівні; на транспортному рівні; на сеансовому рівні; на презентаційному рівні; на прикладному рівні;
	3) НСД до інформації користувачів або технологічної інформації залежно від способу доступу: загрози НСД до операційного середовища (до команд, інструкцій); загрози дії на технологічну інформацію, не пов’язані з допуском порушника до команд операційної системи (відмова в обслуговуванні при перевантаженні, збій операційної системи); загрози програмно-математичної дії;

Загрози інформаційній безпеці СУ КСІІ є цілями/кінцевими результатами діяльності порушників інформаційної безпеки.

V Аналіз загроз інформаційній безпеці СУ КСІІ

Аналіз загроз інформаційній безпеці СУ КСІІ дозволяє виділити складові сучасних комп'ютерних загроз – їх джерела та сили, що їх рухають, способи і наслідки реалізації. Аналіз виключно важливий для отримання всієї необхідної інформації про інформаційні загрози, визначення потенційної величини збитку, як матеріального, так і нематеріального, і вироблення адекватних заходів протидії.

При аналізі загроз інформаційній безпеці СУ КСІІ використовуються три основні методи:

пряма експертна оцінка;

статистичний аналіз;

факторний аналіз.

Розглянемо наведені методи докладніше:

Пряма експертна оцінка. Метод експертних оцінок заснований на тому, що параметри загроз задаються експертами. Експерти визначають переліки параметрів, що характеризують загрози інформаційній безпеці, і дають суб'єктивні коефіцієнти важливості кожного параметра.

Статистичний аналіз – це аналіз інформаційних загроз на основі накопичених даних про інциденти інформаційної безпеки, зокрема, про частоту виникнення загроз певного типу, їх джерела і причини успіху чи неуспіху реалізації. Наприклад, знання частоти появи загрози дозволяє визначити ймовірність її виникнення за певний проміжок часу. Для ефективного застосування статистичного методу потрібна наявність досить великої за обсягом бази даних про інциденти. Потрібно відзначити ще одну вимогу: при використанні об'ємних баз необхідні інструменти узагальнення даних і виявлення в базі вже відомої та нової інформації.

Факторний аналіз заснований на виявленні факторів, які з певною ймовірністю ведуть до реалізації загроз і тих або інших негативних наслідків. Такими факторами можуть бути наявність привабливих для кіберзлочинців інформаційних активів, уразливості СУ КСІІ, високий рівень вірусної активності в зовнішньому середовищі і т. д. Оскільки на сучасні інформаційні системи впливають безліч факторів, зазвичай використовується багатофакторний аналіз.

VI Висновок

З урахуванням викладеного, при розробці заходів щодо забезпечення безпеки інформації, контролю та підготовки вихідних даних для оцінки ефективності вжитих заходів і засобів захисту інформації СУ КСІІ при

аналізі загроза інформаційній безпеці найбільш ефективно застосовувати комплекс різних аналітичних методів для визначення переліку актуальних загроз безпеці інформації для конкретної СУ КСІІ. Це значно підвищує точність оцінки.

Список використаної літератури: ***1.****Guide to BS 7799 risk assessment and risk management. – DISC, PD 3002, 1998 [Електронний ресурс]. – Режим доступу: www.riskserver.co.uk/bs7799.* ***2.*** *Guide to BS 7799 auditing – DISC, PD 3004, 1998 [Електронний ресурс]. – Режим доступу: www.riskserver.co.uk/bs779. 3. ISO 15408 [Електронний ресурс]. – Режим доступу http://www.iso.org/iso/home/search.htm?qt=15408&sort=rel&type=simple&published=on.*